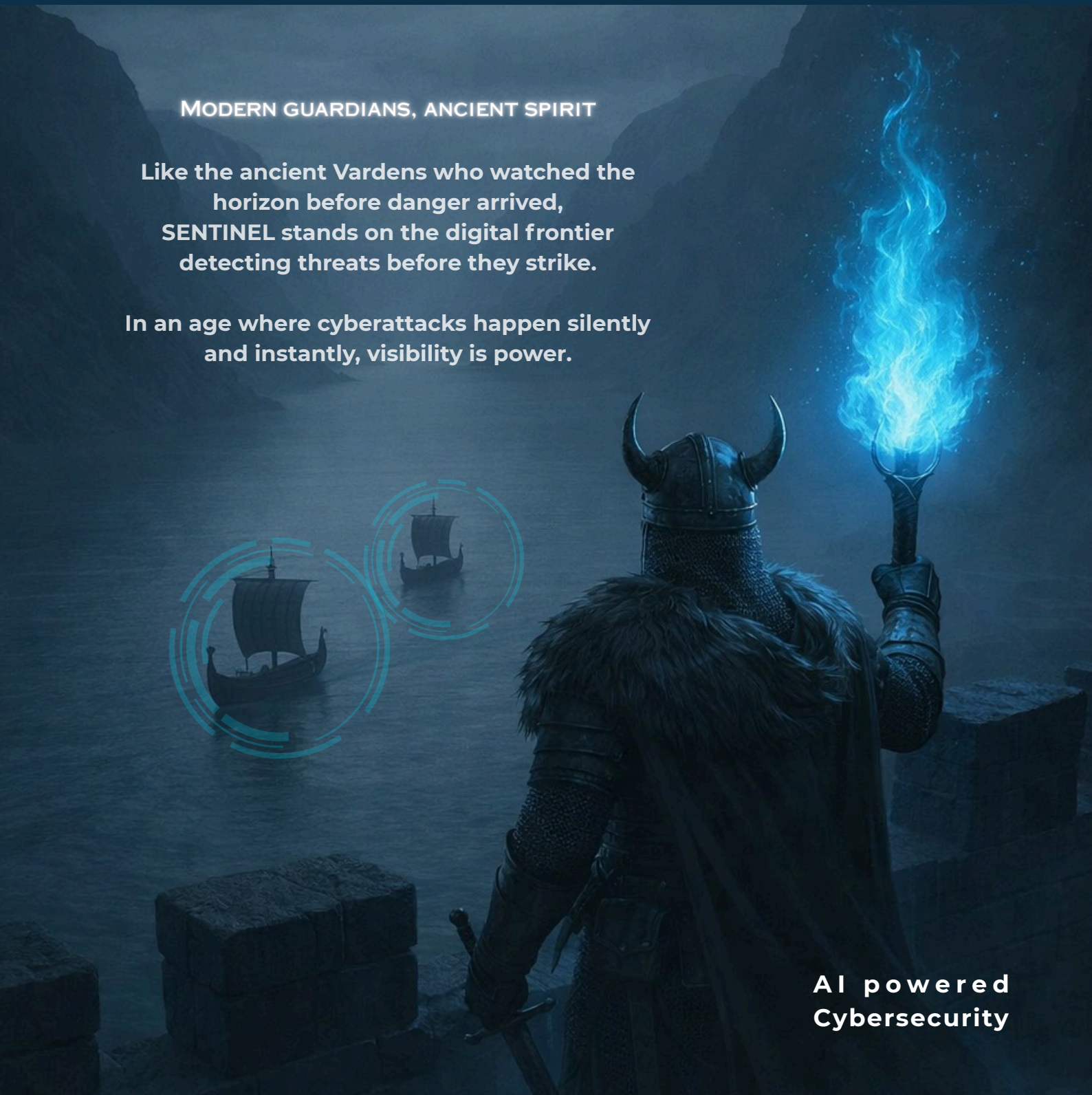
VARDEN security

presents

VARDEN SENTINEL

Automated cyber risk testing platform

The first accessible, **AI-powered cyber guardian** for your organization.



In a world where **cyber threats outpace security resources**, organizations need **AI** to optimize visibility and control.

Varden Sentinel is an AI-driven cyber diagnostics platform that automatically analyzes exposure, interprets vulnerabilities, and translates technical risk into clear, business-ready decisions-making advanced security **diagnostics accessible to all.**

Pentesting is the first technical diagnosis of an organization :

- Before policies.
- Before compliance.
- Before investments.

Yet for many organizations, it remains :

- expensive,
- complex,
- inaccessible,
- or postponed...

Varden Sentinel solves that by bringing pentesting accessible to every organization.

- In 2023, external penetration tests uncovered 34 % of vulnerabilities as critical or high risk (Positive Technologies, Pentesting Results for 2023).
- 72 % of organizations reported that penetration testing had helped prevent an actual security breach (Core Security, 2024 Penetration Testing Survey Report).
- In 85 % of organizations, pentesters detected password policy flaws, while in 60 %, they identified high-risk vulnerabilities linked to outdated or unsupported software (Pentest-Tools.com, Penetration Testing Statistics, aggregating multiple industry studies)

Varden Sentinel automatically **simulate attacks** on your infrastructure, applications, networks, systems, APIs to reveal hidden weaknesses that real adversaries could find and exploit.

A **penetration test** is more than a vulnerability scan: it's an intentional, adversarial approach that tests not just what's wrong, but how far an attacker could go.

Varden Sentinel exploits chains of vulnerabilities (e.g. phishing + weak credentials + misconfiguration + outdated & vulnerable software + database vulnerabilities...) to expose the impact (data exfiltration, lateral movement, privilege escalation). Then, it delivers a **prioritized roadmap** so you can remediate the most critical issues first.

Designed for NIS2 and modern governance

Sentinel supports organizations in:

- risk identification
- technical exposure assessment
- evidence-based security planning
- demonstrating cyber maturity

VARDEN SENTINEL

Three levels. **One** mission: **make cyber risk visible.**

Varden Sentinel
The AI-powered cyber diagnostic platform

- Comprehensive asset inventory
- Technology stack identification for each asset
- Configuration assessment of assets
- Vulnerability identification
- Technology-specific vulnerability reporting
- Executive and technical summaries
- Prioritized remediation roadmap

Target organizations:
- SMEs and mid-sized companies
- Public institutions and municipalities
- Organizations subject to NIS2 requirements
- Boards and executives seeking objective cybersecurity insight

Advantages:

- **Budget control**: predictable pricing with no hidden costs, easily integrated into annual or multi-year financial planning.
- **Full configurability**: choice of scope, testing frequency, and depth based on your needs and security maturity.
- **Scalability** over time: the ability to progressively increase protection as your organization grows or as risks evolve.

LEVEL 1 : OSINT:
What the world already knows about you

Analysis based exclusively on publicly available information.

Reveals:
- exposed systems and domains
- known vulnerabilities
- reputation risks
- leaked or indexed technical data

LEVEL 2 : PASSIVE
What your infrastructure reveals

Advanced reconnaissance without touching internal systems.

Reveals:
- subdomains & DNS structure
- hosting and third-party exposure
- architecture weaknesses
- surface attack mapping

LEVEL 3 : ACTIVE
What machines can technically exploit

Automated controlled scans that detect real technical weaknesses.

Reveals:
- misconfigurations
- vulnerable services & software
- SSL/TLS weaknesses
- CMS & web vulnerabilities
- exposed sensitive files

Want to learn more about Varden Sentinel?

Discover how continuous, configurable penetration testing can strengthen your security posture.

Get in touch to request more information or a tailored demo.

Our expertise:

1. Penetration Testing — Identify vulnerabilities before attackers do

Our pentesting services follow a progressive framework to meet every security maturity level:

- One-time Pentest — a focused security audit to detect vulnerabilities.
- Pentest + Fix & Validation — we correct the vulnerabilities and verify remediation.
- Custom Pentest — tailored scenarios, including advanced red-team testing.

2. Cyber Protection — Secure your networks, systems, data & supply chain

Our system protection services strengthen your digital infrastructure through:

- EDR (Endpoint Detection & Response) — advanced endpoint defense.
- XDR (Extended Detection & Response) — unified threat detection across all layers.
- Secure storage — data encryption, controlled access.
- BCP / DRP — Business Continuity and Disaster Recovery Plans.

3. Compliance & Governance — Ensure regulation standards

We help your organization meet European and international cybersecurity requirements through:

- Risk assessments and gap analysis for AI act, CRA, NIS2, GDPR, ISO 27001, DORA...
- Tailored compliance roadmaps and continuous improvement frameworks.
- Policy development and risk governance models aligned with your business processes.

4. Varden Academy, awareness & Trainings — Empower your teams against human error

Our awareness programs combine OSINT-based spear-phishing and custom training campaigns:

- Controlled phishing campaigns using Varden's secure delivery systems.
- Targeted OSINT data collection to craft realistic test scenarios.
- Varden Academy empowers your teams and human cyber skills

5. Monitoring — Detect threats, respond fast, and ensure security of your systems

We ensure continuity through proactive monitoring and recovery strategies:

- Continuous threat monitoring and anomaly detection.
- Varden Sentinel — AI-powered penetration platform.

www.varden-security.eu
contact@varden.io
Axel: +32470478806
Stéphane: +32495267506
Mathieu: +32477357176

Editeur responsable Mathieu Michel, rue Saint Urbain, 5 - 1370 Jodoigne